REMARKS/ARGUMENTS

The present application discloses a document repository system in which the originator of the document is able to ensure the integrity and security of its document filed with a third party repository without having to trust the administrator of that repository. In this repository system, the document originator and the repository administrator have vault environments which are secure extensions of their respective work spaces. The vault of the document originator encrypts a document that it receives from the originator, prior to forwarding it on to the vault of the repository to maintain the document secure from the repository administrator. When a request is made to view the document, it is made from the vault which is a secure extension of the requesting party's work space to the repository's vault. The repository's vault retrieves a copy of the encrypted document which is forwards, along with the requester's identity, to the originator's vault. The originator's vault verifies that the requester is authorized to view the document from the access control list using an access control list identifying access ownership privileges for the document stored in the vault itself. The originator's vault decrypts the document and forwards the decrypted document directly to the requester's vault. Therefore the repository administrator never handles the decrypted documents or the encrypting and decrypting of the documents.

The repository system also maintains the information on authorized user access secure from any actions of the third party administrator of the repository. To this end, the system includes a communications environment that houses a first agent program in the data repository system which is a secure extension of the work space of the depositor's computer and a second agent program which is a secure

extension of the work space of a first user computer with access privileges to the electronic data file. The first user computer has a record of its access privileges to the electronic data file which is accessible to and maintained by the second agent program. When changes are made to the manifest affecting the first user computer's access privileges to the electronic data file, these changes are communicated from the first agent program to the second agent program so that the first user computer's record of its access privileges can be updated. The first agent program is also able to verify the first user computer's access privileges to the electronic data file before the electronic data file is released to the second agent program.

Claim Rejections Under 35 USC 102

Claims 1, 3-4, and 6-15 in the application were all rejected under 35 USC 103(a) as being unpatentable over the Frisch reference entitled "Essential system Administration" 2nd Edition in view of Garfinkel Practical UNIX Security, both references being published by O'Reilly & Associates, Inc.

As pointed out previously, page 226 of the Frisch reference discusses the system administrators ability to grant "root" access to an account. Therefore, the administrator could grant him/herself such access. Further, material beginning on page 246 of the Frisch reference makes it clear that the repository administrator has access to directory when running a program called "crack". Therefore the repository administrator in a third party repository would have access to the user's account and its directory. Further, the Examiner points out that the Frisch patent does not "disclose means of establishing a secure extension of each computer of a plurality of computers." Relying on the Garfinkel article, the Examiner argues that

NFS affords such a secure extension for NFS mounted file systems. However, that article, particularly its last two pages, makes it clear that materials resident in an NFS system are not too secure and recommends that if concerns about security are paramount perhaps the user should not use NFS. Furthermore, the applicant's attorney found nothing in the Garfinkel article about restricting the access set forth in the Frisch reference of a repository administrator to a directory of authorized users for data stored in the repository. Certainly there is nothing in the Garfunkel article teaching the above described way of restricting an administrator's access. For those reasons the combination of the Frisch and Garfunkel articles does not teach the above described manner of restricting of the administrators ability to enter the user's account and get access to its directory nor does it suggest, to those skilled in the art, modification of the Frisch reference as proposed by the Examiner.

All claims in the application are allowable over the Frisch and Garfinkel references for the reasons discussed above. For instance, claim 1 calls for a system restricting access by the repository system administrator to lists of access privileges to electronic data files of a document depositor. Independent claims 9, 10, 11 and 14 calls for a data repository in which data and the directories for that data are secure from the repository administrator. Dependent claims further distinguish from the prior art.

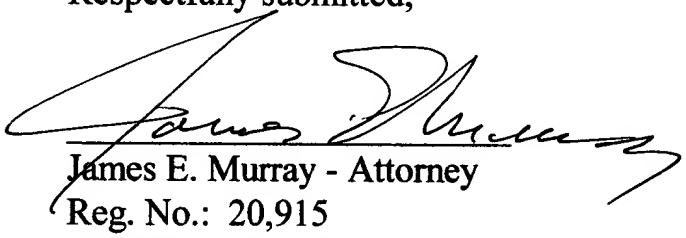
Allowable Subject Matter

The Examiner has stated that dependent claim 16 would be allowable in independent form. Applicants have placed the subject matter of claim 16 in independent form as claim 17, including all subject matter contained in independent

claim 14 and intervening dependent claim 15. For this reason, claim 17 should be allowable. New claims 19 and 21 should be allowable for the same reason as new claim 17 since they incorporate subject matter contained in dependent claim 16.

For the above reasons, it is respectfully submitted that the claims are allowable over the prior art and the application is in condition for allowance. Therefore, it is requested that the application be reconsidered, allowed and passed to issue.

Respectfully submitted,



James E. Murray - Attorney
Reg. No.: 20,915
Telephone No.: (845) 462-4763